(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

WO 01/98970 A1

(54) Title: A SYSTEM FOR NOTIFYING USERS IN REAL TIME OF TRANSACTIONS UNDERTAKEN

(57) Abstract: A security system for notifying users in real time of financial transactions executed, having a software platform including a data server, a domain name server, and communications program is provided. The system directly connects users (11) to the database (15) that records their transactions. It transfers the transaction information of recently executed transactions from the database of the financial institution to the Web (19), Internet Service Provider (19), cellular provider (18), paging service (20) etc. of the user. For example, the transaction information from an executed transaction (12) may be sent in real time to the user's email, pager, PDA or cellular phone or any other Internet enabled device chosen by the user. In this way, the user is able to monitor actual usage of his or her financial tools such as credit cards, checks and money transfers and may respond to unauthorized or incorrect usage within minutes or even seconds.

A SYSTEM FOR NOTIFYING USERS IN REAL TIME OF TRANSACTIONS UNDERTAKEN

5

FIELD AND BACKGROUND OF THE INVENTION

The present invention relates to a system for notifying users in real time of transactions undertaken both online and offline.

Security problems have always been one of the primary factors in dissuading

10 buyers to part with their money when purchasing from various sources and in various ways. The history of finance has been a continual battle between users of financial currency and criminals. As technology has enabled new ways to conduct transactions, so have criminals found new ways to break through the security apparatus and steal funds. The credit card industry, for example, has become one of the primary ways of executing

15 transactions. Owing to their ease of use, international acceptability and flexibility of use, they are used both offline and online by hundreds of millions of people worldwide.

However, as with all other transaction methods, thievery is rife, as thieves that can attain valuable card information or that use lost or stolen cards can easily abuse the system and steal money. It has been estimated that in the U.S.A. in 1999, thefts from

20 credit card transactions at VISA alone were $1,700,000,000. The inception of e-commerce has introduced a tremendous number of new buying channels, but the concerns with maintaining security when purchasing are ever present. By far the most common method of purchasing online is by using credit cards. With this use of Credit Cards

online, thieves and hackers have been able to break in on the buying cycle, stealing

25   money from online sales, and causing great suspicion among potential buyers. It is

estimated that only 30% of U.S.A Internet users have executed transactions online. For e-

commerce to succeed, however, buyers will need to be more certain that there will be

reasonable security and privacy. The entire buying chain, from the buyer, to the financial

companies, to the sellers, will need to prove that money passing between them will be

30   secure and that theft will be prevented. The stakes are thus extremely high, both in terms

of stolen money and lost revenue, to find a solution to the theft that occurs during the

transaction processes both online and offline.

Various attempts have been made to ensure security when executing transactions

both online and offline. Offline security, in the case of credit card usage, is usually

35   limited to the seller phoning the credit card company to verify the card and buyer details

before permitting the sale to go ahead. This method is relatively secure if the buyer is

actually present and shows an identity document, however this is generally not the case.

Moreover, transactions of this type take place constantly when buying telephonically,

where the buyer may be anyone who has managed to find the necessary credit card

40   details. Furthermore, this method of security simply ensures that payment is permitted in

terms of there being money in the credit card account and the card has not been reported

stolen – but does not at all guarantee that the person buying is actually the legitimate

credit card holder. The same limitations exist in cases where the verification occurs

automatically. Other solutions have been proposed that use new technologies to verify

45   users or buyers. These include biological solutions such as recognition by fingerprint or

by retina. Once again, the same problem exists – that besides being expensive and

difficult to setup and maintain, once a theft occurs, the user may not know about it for

some time. The time after the theft is the critical element that needs to be dealt with.

Online commerce has other technology solutions, however all known current buying

50   procedures and security methods revolve around preventing credit card details or other

critical purchasing information from falling into the wrong hands. For example Secure

Server technology, such as Secure Sockets Layer (SSL), aims to manage the security of

message transmissions in a network. A security layer stands in front of the transaction

process, allowing only authorized sales to proceed. Once again, this type of security

55   method aims to limit information leakage by scrambling credit card information, so that

information entered into a users computer will not be leaked to other than the desirable

destination. The common denominator among all the systems currently known is the

prevention of credit cards or other critical information being discovered and used without

authority of the owner. There are, however, no known systems that effectively deal with

60   actual knowledge of when unauthorized transactions have occurred and therefore being

able to monitor and respond to unauthorized usage in a highly effective way.

In spite of all the attempts by financial institutions to prevent theft, possibly one

of the fundamental reasons for its proliferation is that invariably, people conducting

financial transactions are not immediately notified by the actual financial institution as to

65   the execution of those transactions. For example, when checks are processed, stocks

bought, or purchases executed, the buyer is usually required to initiate contact with his or

her financial institution in order to confirm the transaction. This is if the buyer wants to

acquire relatively updated information, as opposed to waiting for mail from the bank etc.

at the end of the month. In terms of security, the time gap between the actual execution of

70   a transaction, and the time that the information is passed on to the buyer is critical in

order to minimize theft.

There is thus a widely recognized need for, and it would be highly advantageous

to have, a system that can notify users about actual financial transactions executed, and

allow for effective, and even real time responses to unauthorized financial usage.

75   The current invention automatically transfers transaction information to the user,

for example to their email or cellular phone. In the preferred way of operating the current

invention, the user is able to monitor actual usage of his or her credit card, and to respond

to unauthorized card usage within seconds or minutes.

80   **SUMMARY OF THE INVENTION**

According to the present invention there is provided a system for notifying users of

transactions executed in real time, comprising:

i)   a data server for storing and transferring transaction information for individual users;

ii) a domain name server for allowing individual users access to their personal

85   information; and

iii) a communications program for automatically sending notifications to various

communications services, applications and devices.

The present invention directly connects users to the database that records their

transactions. It transfers the transaction information of all executed transactions from the

90   database of the credit card companies, banks etc. to the Web, Internet Service Provider,

cellular provider, paging service etc. of the user. For example, this information may be

sent to the user's email or cellular phone, or any other device that is or will be most

accessible and on hand for the user. Another example of how the system may operate is in the case of ticket ordering. In addition to the transaction details being sent to the user,

95 the ticket confirmation information or any other useful information for which the user is waiting, can be sent automatically and in real time to the user. In this way the user is able to monitor actual transactions resulting from usage of his or her credit card, checkbook, bank account, travel agency etc. This will enable the user to respond to unauthorized or incorrect usage of financial instruments within minutes or even seconds, and to be

100 updated in real time regarding any other information that may be transferred electronically and is important to the user.

BRIEF DESCRIPTION OF THE DRAWING

The invention is herein described, by way of example only, with reference to

105 the accompanying drawings, wherein:

The FIGURE is a flow chart of the basic components of the system according to the current invention.

DESCRIPTION OF THE PREFERRED EMBODIMENT

110 The present invention is of a system for notifying users in real time of transactions executed.

Specifically, the present invention can be used to transfer transaction information in real time from the point of sale, via the financial institution, and to the user.

The principles and operations of such a system according to the present invention

115   may be better understood with reference to the drawing, and the accompanying

description, wherein:

The FIGURE illustrates a flow chart of the basic components and operations of

the current invention in its preferred usage, in the case of a credit card transaction. In

order to use the current invention, the credit card companies have to update their legacy

120   systems to incorporate a new computer platform that can provide each credit card holder

an up-to-date personalized page of his or her transactions. This system will include a

database server for user information such as device details and personal preferences, as

well as a domain name server (DNS) that will control the process whereby users may

access their personal pages within the credit card company Website. All the credit card

125   companies have existing databases with client records and information, so the only thing

that needs to be added is for users to have access to this database. Furthermore the credit

card companies will need to ensure that all credit card transactions are executed

electronically, not with a card "iron", so that transaction details will be immediately

transferred to the credit card company database. The credit card holder will possibly be

130   able to access their personal page using a password from inside the credit card company's

Website, in order to monitor transactions executed. In the most effective use of the

current invention, the user will inform the credit card company of his or her personal

preferences regarding how they would like to be informed when transactions occur. For

example the user may want to receive all notifications to their email box or cellular

135   phone, without having to check the credit card company's Website.

In the current example of the preferred functioning of the current invention, the credit card holder **11** uses a credit card to execute a transaction **12** online, offline or via phone. The transaction information is then transferred electronically from the market/web to the credit card company's computer system **14**. The credit card company

140   computer system will incorporate legacy systems, which contain electronic databases of client records and client details. The current invention will simply require of the credit card company to update their systems to display real time updates of personal profiles, and to allow users online access to these profiles. In this way users will be able to access their personal records, such as latest transactions, by entering their personal pages on the

145   credit card company Website. Part of the updating process should be that the credit card company encourage only electronic payments, as to the exclusion of credit card irons for example, so as to ensure that all transactions executed can be registered and transferred to the credit card holder instantaneously. The second addition that the current invention will make to the existing financial institution systems will be the ability to forward the

150   relevant personal information. For example, the credit card company database will need to recognize the relevant information, such as critical information of the most recent transaction, and send it automatically to various devices or applications such as the user's email box, cellular phone, pager, PDA or any other device that is or will be most accessible and on hand for the user. This will require a simple updating of the current

155   credit card company computer systems, such as fields for contact details and personal preferences, so that the system will be able to determine to which device or application to send the chosen information. The updated system will require basic communication software to enable forwarding of this information, or notifications, to various types of

8

160   Internet enable devices, applications and services. This system update is referred to as the new data server. The credit card company's new data sever **14** will automatically update the credit card holders' personal pages **15**, whether the user has access to this page or not.

The credit card company's computer system **14** then automatically sends a quick and instant message **17** to either the credit card holder's cell-phone/pager etc. company **18**, or the ISP or a Webpage-based source **19**. From these sources the messages are

165   automatically forwarded to the credit card holder's cellular phone, pager, PDA, Facsimile etc. **20** or whatever relevant device or application the credit card holder decided. Alternatively, the message may be forwarded to a Webpage-base program or client program on a personal computer, such as email, instant messaging, etc. **21**. This process entails cooperation between various communication providers, such as internet service

170   providers (ISP's), cellular phone companies, pager companies etc., in order to complete the communications network so that the relevant notification can be transferred from the credit card company database to the chosen device or application.

Once a notification is received, for example on a cellular phone, the credit card holder is alerted and can then view the notification. In the case where an unauthorized

175   transaction was made, the credit card holder can immediately contact the credit card company's security office **16** in order to cancel the card. Alternatively, the credit card holder may opt to check his or her transactions on his or her personal Webpage on the credit card company's Website **15**.

Another example of how the current invention may operate is in the case where a

180   credit card holder receives messages via e-mail. He or she can order his or her Internet service provider to forward the relevant messages to his or her cellular phone. There may

be any number of communications and collaborations between various communication

devices, Internet services and applications, and applications that are capable of receiving

notifications via the Internet.

185   If the credit card companies will not accept the accessing of personal pages on

their sites due to security concerns, then the same process will be undertaken, without the

option for individuals to access their information on the credit card company Website.

The relevant information will simply be forwarded to the relevant communications

device, service or application. For example, the user may instruct the credit card company

190   to forward all credit card transactions to his or her cellular phone, and this will be

executed in real time without the need for the user to access any Website.

In another aspect of the invention, a credit card holder's e-mail address, and/or

information pertaining thereto, is disposed on the credit card. In current, magnetic-stripe

type credit cards, the information is preferably provided as digital information within the

195   magnetic stripe. Upon making a transaction, the platform at point of sale **12** is designed

and configured to read this e-mail address and automatically send a quick and instant

message **17** to credit card holder's cell-phone/pager etc., company **18**, to ISP or

Webpage-based source **19**, or to any automatic-type messaging service.

In a preferred embodiment of the present invention, the platform at point of sale

200   **12** transfers the transaction data to credit card company **13**. Credit card company **13**

subsequently transmits to the platform at point of sale **12** (in addition to conventional

information) the e-mail address of the credit card holder, which is preferably stored

within a data bank of credit card company **13** or in any data storage area to which credit

card company **13** has access. The platform at point of sale **12** is designed and configured

205   to, after receiving this address, automatically send a quick and instant message **17** to

credit card holder's cell-phone/pager etc., company **18**, to ISP or Webpage-based source

19, or to any automatic-type messaging service. From these sources, the messages are

automatically forwarded to the credit card holder's cellular phone, pager, PDA,

Facsimile, etc. **20** or to any device or application specified by the credit card holder.

210   Alternatively, the message may be forwarded to a Webpage-based program or client

program on a personal computer, such as email, instant messaging, etc. **21**.

In this fashion, the computer system of credit card company **13** is better isolated

from the various above-described information-receiving units such as credit card holder's

cell-phone/pager etc., company **18**, ISP or Webpage-based source **19**, and/or a Webpage-

215   based program or client program on a personal computer, such as email, instant

messaging, etc. **21**. This is particularly advantageous in that the computer system of

credit card company **13** is significantly more secure than in configurations in which

computer system of credit card company **13** deals directly with such information-

receiving units.

220   With this new service and system, the credit card holder will be alerted within

minutes or even seconds of all transactions executed, and can react immediately to stop a

thief using his or her credit card after or even during the first unauthorized transaction.

This is achieved by simply contacting the credit card company security officer and

ordering to cancel the credit card immediately.

225   An additional use of the current invention may be to transfer real time

notifications to travelers, prizewinners etc. The legacy systems of a travel company, for

example, can update their system with the data server and communications program of

the current invention, and ensure that clients are notified as soon as tickets have been confirmed. In this way clients waiting for critical and timely travel information can be

230 notified immediately upon the information being available, and will be available to respond promptly to incorrect or unauthorized transactions.

While the invention has been described with respect to a limited number of embodiments, it will be appreciated that many variations, modifications and other applications of the invention may be made.

WHAT IS CLAIMED IS:

1. A system for notifying users in real time of financial transactions executed,

   comprising a software platform including:

   a data server for storing, filtering and transferring financial transaction information;

and

   a communications program for sending real time notifications of said transaction

information from recently executed financial transactions, to various communications

services, applications or devices as defined by the user.

2. The system of claim 1, wherein said financial transactions include purchases by credit

   card, smart card, check, money transfer, cyber-cash or any other type of transactions

   where transaction information can be transferred electronically.

3. The software platform of claim 1, wherein said data server includes a domain name

   server for accessing personal profiles.

4. The software platform of claim 1, wherein said data server includes personal contact

   information and transaction information.

5. The software platform of claim 1, wherein said communications services, applications

   and devices include products selected from the group consisting of telephones,

   cellular phones, Web phones, PDA's, pagers, PC's, notebook computers, email,

   instant messaging, Internet enabled gadgets, Internet enabled appliances and any

   other communications device, service or application.
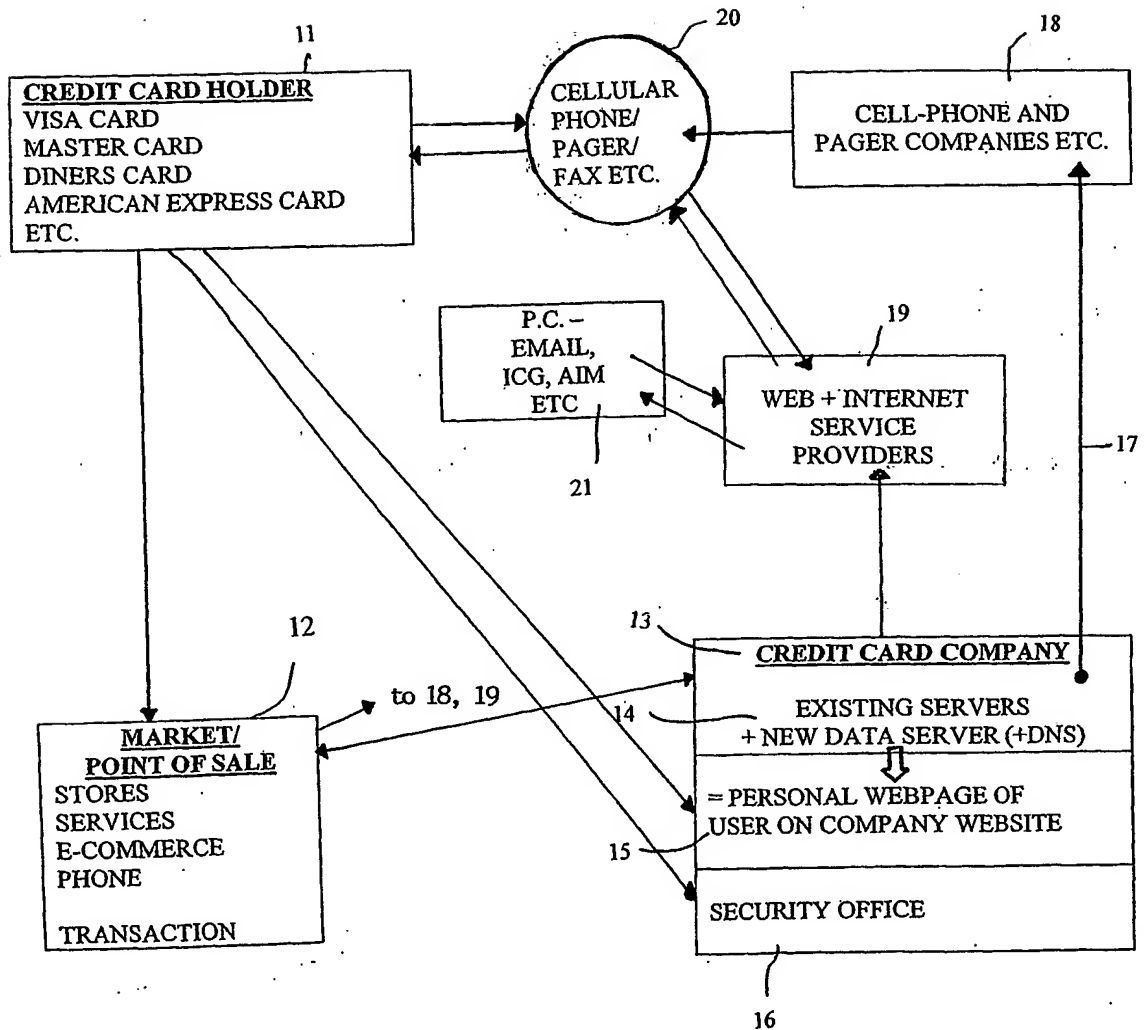
INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL 01/00569

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7)   :GO6F 17/60
US CL   :705/39
According to International Patent Classification (IPC) or to both national classification and IPC

B.   FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. :   705/1, 35, 38-42

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C.   DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,842,185 A (CHANCEY ET AL.) 24 NOVEMBER 1998, SEE ENTIRE DOCUMENT.	1-5
A	US 5,649,115 A (SCHRADER ET AL.) 15 JULY 1997, SEE ENTIRE DOCUMENT.	1-5
A	US 4,948,174 A (THOMSON ET AL.) 14 AUGUST 1990, SEE ENTIRE DOCUMENT.	1-5
X	JP 10269003 (SEIJI KURAYA) 09 OCTOBER 1998, SEE ENTIRE DOCUMENT.	1-5

☐ Further documents are listed in the continuation of Box C.   ☐   See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance		
"E"	earlier document published on or after the international filing date	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)		
		"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed	"&"	document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 OCTOBER 2001	**21 NOV 2001**

Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	Authorized officer FRANTZY POINVIL
Facsimile No. (703) 305-3230	Telephone No. (703) 305-9779

Form PCT/ISA/210 (second sheet) (July 1998)★

THIS PAGE BLANK (USPTO)